SHEPPARD MULLIN RICHTER & HAMPTON LLP
JAY T. RAMSEY Cal. Bar. No. 273160
1910 Avenue of the Stars, Suite 1600
Los Angeles, California 90067-6055
Telephone: 310.228.3700
Facsimile: 310.228.3701
Email: jramsey@sheppardmullin.com

KLEIN, MOYNIHAN, TURCO LLP
NEIL ASNEN (Admitted Pro Hac Vice)
450 7th Ave.
New York, New York 10123
Telephone: 212.246.0900
Email: nasnen@kleinmoynihan.com

Attorneys for Defendant What If Holdings, LLC d/b/a C4R Media Corp.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION

LORETTA WILLIAMS, individually and on behalf all others similarly situated,

Plaintiffs,

v.

WHAT IF HOLDINGS, LLC d/b/a C4R MEDIA CORP., and ACTIVEPROSPECT, INC.

Defendants.

Case No. 3:22-cv-3780-WHA

Assigned to the Hon. William Alsup

DEFENDANT WHAT IF HOLDINGS, LLC d/b/a C4R MEDIA CORP.'S MOTION TO COMPEL ARBITRATION AND/OR DISMISS

Date: December 14 2022
Time: 8:00 a.m.
Courtroom: 12, 19th Floor

Complaint Filed: June 27, 2022
Trial Date: None Set

Table of Contents **Page**

Table of Authorities

Statutes

Defendant What If Holdings, LLC ("WIH" or "Defendant") respectfully submits the following reply memorandum of points and authorities in further support of its Motion to Compel Arbitration and/or Dismiss (the "Motion")

I. INTRODUCTION

Plaintiff's Opposition to Defendant's Motion serves to highlight the herculean challenges facing marketing companies that attempt to comply with the state and federal regulatory framework governing telemarketing. On the one hand, the federal dockets are clogged with lawsuits claiming that individuals have received telemarketing calls or messages without their consent in violation of the Telephone Consumer Protection Act 47 U.S.C. § 227 *et seq.* ("TCPA"). When presented with evidence of that consent, plaintiffs often dispute the authenticity or reliability of that record evidence. Now, when digital marketing companies engage with vendors to provide authentication and verification of the record evidence which TCPA plaintiffs claim had been lacking, digital marketing companies are accused of facilitating illegal wiretapping for no other reason than the fact that those vendors have technological capabilities which they themselves lack. Orwell himself would blush at the efforts to turn compliance practices into purported violations of law.

Nevertheless, Plaintiff's efforts prove futile as (i) she consented to the recording of which she complains; and (ii) her allegations fail to state a claim for which relief may be granted. This in addition to the fact that she brought her purported claims in the wrong forum, having previously agreed to arbitrate any claims

concerning the subject website. The Court should thus grant Defendant's Motion accordingly.

II. ARGUMENT

A. The Design and Content of Defendant's Website is Not in Dispute and Gives Rise to an Enforceable Agreement

Courts in this Circuit applying California contract law have consistently held that all that is needed for a user to manifest assent to a browsewrap agreement is for the user to be presented with information that would put a reasonably prudent user on inquiry notice of the terms. Defendant's notice is more than sufficient under this standard and Plaintiff's heavy reliance on the decision in *Berman v. Freedom Fin. Network LLC*, 2020 WL 5210912 (N.D. Cal. Sept. 1, 2020) does nothing to alter this truth. In fact, where the *Berman* court found shortcomings with the notice presented to it, Defendant's website differs in material ways, is materially distinguishable, and thus ultimately satisfies the standards necessary to give rise to an enforceable contract.

As an initial matter, *Berman* noted that it is permissible to disclose terms and conditions through a hyperlink but reinforced the notion that the design of the hyperlink must put a user on notice of its existence. *See Berman v. Freedom Financial Network, LLC*, 30 F.4th 849 (9th Cir. 2022). In *Berman*, the webpage's terms and conditions hyperlink, while underlined, was in the same grey font color as the disclosure notice within which it was located. In contrast, here, the hyperlink was highlighted in blue, "the color typically used to signify the presence of a hyperlink." *Id.* at 854. Moreover, this blue hyperlink conspicuously stood out among the black

fonted text among which it was located. Plaintiff would not have been required to hover her mouse over otherwise plain-looking text or aimlessly click on words on a page to ferret out a hyperlink on this webpage. *Id.* at 857. To the contrary, this webpage used bright blue words that stand out among the surrounding text to indicate that a user understands that "Terms and Conditions" is a hyperlink. Moreover, both the Terms and Conditions hyperlink and the disclosure language pursuant to which Plaintiff assented are located directly above the only button on the webpage. Its proximate location to that button makes it impossible for a user such as Plaintiff to not notice it if or when s/he clicks that button, which Plaintiff has acknowledged doing. Finally, the legal significance of clicking the button is explained to users of the webpage by indicating that "[b]y signing up, I agree to the FoundMoneyGuide Privacy Policy and Terms and Conditions…"

Plaintiff seeks to impose a higher standard for enforcement of browsewrap agreements than the law otherwise requires. Nevertheless, in the absence of an affirmative statement such as "By clicking the button I agree" it is sufficient if (1) a user "knew or should have known of the terms" and (2) the circumstances are such that the user "understood that acceptance of the benefit would be construed by the offeror as an agreement to the bound." *Schnabel v. Trilegiant Cor.*, 697 F.3d 110, 128 (2d Cir. 2012). *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171 (9th Cir. 2014) approving citation to *PDC Labs, Inc. v. Hach Co*., 2009 WL 2605270 (C.D. Ill. Aug. 25, 2009) provides a useful example of the sufficiency of Defendant's notice. In *PDC*

Labs, a user was deemed to be bound by website terms when the notice provided "STEP 4 of 4: Review terms, add any comments, and submit order," which was then followed by a hyperlink to the terms. *Id.* at *3. This was deemed sufficient to put a reasonable user on notice that he was agreeing to the terms. "Review terms" is far less explicit that Defendant's notice which explicitly informs the user that "[b]y signing up, I agree to the FoundMoneyGuide Privacy Policy and Terms and Conditions. . ."

It is notable that Plaintiff characterizes this agreement as a "sign in wrap" agreement. The California Court of Appeals has addressed whether "sign in wraps" are "sufficiently conspicuous to bind" plaintiffs to arbitration provisions. In *Sellers v. JustAnswer LLC*, 73 Cal.App.5th 444 (2021), the Court observed that "whether 'sign in wrap' agreements put consumers on sufficient notice, courts consider: (1) the color of the text as compared to the background it appears against; (2) the location of the text and, specifically its proximity to any box or button the user must click to continue use of the website; (3) the obviousness of any associated hyperlink; (4) the size of the text; and (5) whether other elements on the screen clutter or otherwise obscure the textual notice. *Id*. at 473. As part of this analysis, the Court of Appeals has also noted that "he full contact of any transaction is critical to determining whether any particular notice is sufficient to put a consumer on inquiry notice of contractual terms contained on a separate, hyperlinked page." *Id*. at 477. It has separately found that where the "circumstances involve a consumer signing up for an ongoing account,

it is reasonable to expect that the typical consumer in that type of transaction contemplates entering into a continuing, forward-looking relationship governed by terms and conditions." *B.D. v. Blizzard Entertainment, Inc.*, 292 Cal.Rptr.3d 47, 64 (2022). "This is the type of transaction in which federal courts have generally found sign-in wrap agreements enforceable." *Id*. at 64-65.

With this recent guidance from the California Court of Appeals, it is apparent that Defendant's Terms and Conditions are enforceable as "sign in wraps." Plaintiff's Opposition admits that her interactions with Defendant's Website involved her submission of personal information in order to receive the Website's offerings. *Opp.* p. 14. On that basis alone, not only has Plaintiff indicated that the typical consumer would reasonably expect that this transaction would be governed by website terms and conditions, as the Court of Appeals recognized in *Blizzard,* but she has acknowledged that *she* recognized it too. Her choice was to accept the offer of the contract, or if those terms were not acceptable to her, decline to take the benefits being offered to her. *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393 (2d Cir. 2004). Plaintiff admits that she accepted the benefits. She thus agreed to be bound. *See* Cal. Civ. Code § 1589 ("A voluntary acceptance of the benefit of a transaction is equivalent to consent to all of the obligations arising from it, so far as the facts are known, or ought to be known, to the person accepting.").

Nevertheless, for the same reasons that the Terms and Conditions are an enforceable browsewrap agreement, they also satisfy the considerations for qualifying

as an enforceable sign in wrap: the Terms and Conditions hyperlink is bright blue set against a light grey backdrop, that bright blue font prominently indicates that "Terms and Conditions" is a clickable hyperlink, the location of the disclosure and hyperlink is directly above the button which Plaintiff admits clicking to continue using the Website, and the disclosure is located within a prominent box set off from the remainder of the webpage and which serves to highlight the language included therein. Thus, whether analyzed pursuant to principles governing browsewrap agreements or sign in wrap agreements, the Terms and Conditions plainly provided sufficient notice to Plaintiff that her use of the Website manifested assent to those terms. She is thus bound thereby and mandated to arbitrate her claims against Defendant.

B. Plaintiff Fails to Demonstrate a Valid Claim for Violation of CIPA

1. Plaintiff Consented to the Recording

Plaintiff first seeks to avoid dismissal of her claims for alleged violation of California's Invasion of Privacy Act ("CIPA") claims by arguing that she did not consent to the recording notwithstanding express language contained within the Website's Privacy Policy stating to the contrary. Her arguments on this point are twofold. First, she argues that she is not bound by the Privacy Policy for the same reasons that she is not bound by the Terms and Conditions. To this, WIH incorporates its arguments set forth above concerning arbitration as they apply with equal force to the validity and enforceability of the Website's Privacy Policy. Plaintiff also argues,

however, that even if she is bound by the Privacy Policy, that the terms thereof do not constitute prior express consent for purposes of CIPA.

The relevant provisions of the Privacy Policy provide, *inter alia*, as follows:

> Where you provide "prior express consent" within the meaning of the Telephone Consumer Protection Act (47 USC § 227), and its implementing regulations adopted by the Federal Communications Commission (47 CFR § 64.1200) . . . you understand and agree that we may use a third party vendor to record and store your registration and consent for compliance purposes.

Dkt. No. 25-1, Exhibit C.

Plaintiff asks that the Court interpret this otherwise unambiguous language to mean that the consent provided to WIH by a website user only becomes effective upon the provision of TCPA consent. Nevertheless, the operative language of the consent clearly indicates that the contemplated recording, to the extent that one occurs, is to begin with registration, an event separate and apart from the provision of TCPA consent (you understand and agree that we may use a third party vendor to record and store your registration and consent for compliance purposes).

What is made plain by the contractual language is that the storage of the recording is contingent upon provision of TCPA consent, not the recordation itself. The Privacy Policy affords Defendant the option to store a user's TCPA consent in instances "where [they] provide 'prior express consent'" It does not make sense for the permission for recording to be conditioned upon provision of TCPA consent, as the event that the Privacy Policy contemplates recording would have already passed

before it could ever be recorded. Perhaps Plaintiff's argument may make more sense if Defendant's Website purported to obtain a user's assent to the Privacy Policy on the same webpage as that on which an individual provides TCPA consent. In that instance, it could be argued that a recording had begun to take place before an individual had given consent. That is not the case with the Website at issue however, where agreement to the Privacy Policy has already been manifested before a user has reached the TCPA webpage described in paragraphs 21-27 of the Complaint and on which the recording is alleged to have taken place and was provided at a point in time before the recording of the TCPA consent occurs in order to permit the record in compliance with the law. Consequently, contrary to Plaintiff's argument, these facts do not implicate the same "retroactive consent" concerns present in *Javier v. Assurance IQ, LLC*, 2022 WL 1744107 (9th Cir. May 31, 2022).

2. *CIPA Does not Apply to the Facts at Issue*

Plaintiff's remaining arguments in opposition to dismissal of her CIPA claims are equally unavailing. She argues that by not specifying which clause of Section 631(a) she invokes, that Defendant's analysis of the inapplicability of the various prongs of the statute lacks any weight. This is little more than a red herring to draw attention away from the fact that much of the statute is simply inapplicable to the facts as pled. Defendant demonstrated that the first prong of CIPA is limited solely to communications passing over telegraph or telephone wires and that Plaintiff's interactions with Defendant's Website does not implicate that prong of CIPA. *Mastel*

v. Miniclip SA, 549 F.Supp.3d 1129, 1136 (E.D. Cal. 2021). Plaintiff effectively concedes this point by instead focusing on whether or not the communication was intercepted while in transmission. Nonetheless, that does not address the fundamental issue that this communication was not transmitted over telephone line.

Instead, Plaintiff's implicit argument is that only CIPA's second clause is plausibly applicable to the instant facts. On this, Defendant is in agreement given that the first prong plainly does not apply and the third prong (to use or communicate information obtained) likewise plainly does not apply as there is no allegation that information recorded was used or communicated. In fact, Plaintiff admits that the recordings are stored only for purposes of compliance with federal law.

This leaves only the second prong of CIPA, to which Plaintiff argues that the keystrokes, mouse clicks, and personal information that she voluntarily submitted to Defendant's website, which have been recognized as record information in myriad previous cases, actually constitutes content for purposes of CIPA. However, the issue of whether recordings made by session replay software similar to that provided by ActiveProspect, Inc. used on a defendant's website can give rise to a wiretapping claim is not a matter of first impression for the courts. In *Graham v. Noom, Inc.*, 533 F.Supp.3d 823 (N.D. Cal. 2021), *Yale v. Clicktale, Inc.*, 2021 WL 1428400 (N.D. Cal. Apr. 14, 2021), and *Johnson v. Blue Nile, Inc.*, 2021 WL 1312771 (N.D. Cal. Apr. 8, 2021), the courts have each addressed the issue of whether session replay software's recording of a website user's interactions on a website violate CIPA. In all three

instances, the courts dismissed the plaintiff's claims. In *Johnson* and *Yale*, the Courts found that the collected information at issue contained record information that is not protected by the statute, while also agreeing with the reasoning of the *Noom* court that the session replay software provider was not an eavesdropper, but rather a vendor which provides software services which allow its clients to monitor the web traffic interactions on its own websites, no different than ActiveProspect and Defendant. Plaintiff has provided this Court with no cause to deviate from these reasoned holdings. The claims should be dismissed accordingly.

C. Plaintiff's Constitutional Claim Lacks Merit

Plaintiff's primary opposition arguments in opposition to dismissal of her purported constitutional claim for alleged violation of the right to privacy is that Defendant's Motion cannot be resolved at the pleading stage. The California Supreme Court has nonetheless counseled otherwise. In fact, it has "instructed that courts have a role to play in 'weed[ing] out claims that involve so insignificant or de minimus an intrusion on a constitutionally protected privacy interest as not even to require an explanation or justification by the defendant." *Loder v. City of Glendale*, 14 Cal. 4th 846, 893 (1997). To that end, if the "undisputed material facts show . . . an insubstantial impact on privacy interest, the question of invasion may be adjudicated as a matter of law." *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 37, 40 (1994).

As noted in Defendant's Motion, to aid in this weeding out process, courts search for an objective criterion to analyze the sufficiency of the constitutional right

to privacy claim notwithstanding a general hesitance to make empirical judgments as to what conduct is egregious, offensive, or violative of societal norms. That objective criterion is whether "the plaintiff alleges that the defendant used the private or confidential information obtained for some improper purpose. *Mastel*, 549 F.Supp.3d at 1140.

Owing to the foregoing, while Defendant vigorously disputes that Plaintiff either had a reasonable expectation of privacy in basic identifying information which she voluntarily provided to Defendant or that recording Plaintiff's voluntary provision of such information constitutes an egregious, offensive breach of societal norms, what is objectively beyond dispute is that the use of such records was in furtherance of practices designed to comply with the TCPA. *Complaint* ¶ 5. This is an eminently appropriate purpose to use the recorded personal information, in stark contrast to the profit seeking marketing purposes sometimes found to inappropriate implicate the right to privacy.

The Complaint does not allege that the records were used for any other purpose, let alone any improper purpose. This is because Plaintiff's pleading accurately observes that the *only* purpose of recordings was compliance related. As a result, Plaintiff's claims are easily distinguishable from the cases which she cites for the proposition that her claims cannot or should not be dismissed at the pleading stage. For example, in *Hart v. TWC Product and Technology LLC*, 526 F.Supp.3d 592 (N.D. Cal. 2021) the allegations specifically asserted that the subject data was collected and

maintained for sale to third parties for advertising and marketing purposes (and in contrast to allegations that the subject defendant explicitly told website users the data would only be used to provide personalized local weather information). Similar improper purposes were alleged in both *Revitch v. Moosejaw, LLC*, 2019 WL 5485330 (N. D. Cal. Oct. 23, 2019) and *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 539 (9th Cir. 2020) in which the plaintiff in *Revitch* alleged that code was embedded on a website which allowed defendants to scan a user's computer for files to de-anonymize and identify the user to obtain anonymous website users' names, home address and detailed browsing histories, *see Revitch*, 3:18-cv-06827 Dkt. 43 ¶1, while the allegations in *In re Facebook* concerned Facebook's use of cookies to track a user's data even after logging out of his/her Facebook account, in order to receive and compile their personally identifiable browsing history, no matter how sensitive the website visited to create a "cradle-to-grave profile" of users without their consent.

In the absence of any allegation that the data acquired by Defendant was used for an improper purpose, the Court is provided the necessary objective criteria necessary to dismiss Plaintiff' constitutional claim for violation of the right to privacy at the pleading stage.

While this alone is enough to dispose of Plaintiff's constitutional claims, Defendant further notes that Plaintiff's allegations show "no reasonable expectation of privacy" and "an insubstantial impact on privacy interests," such that the question

can be adjudicated as a matter of law. *Low v. LinkedIn Corp.*, 900 F.Supp.2d 1010, 1025 (N.D. Cal. 2012) *citing Pioneer Electronics, Inc. v. Sup. Ct. of L.A.*, 40 Cal. 4h 360, 370 (2007). The California Constitution sets a high bar for an invasion of privacy claim. It has been held that disclosure of personal information, including social security numbers, does not constitute an egregious breach of social norms. *In re iPhone Application Litig.*, 844 F.Supp.2d 1040, 1063 (N.D. Cal. 2012). It has further been held that *theft* of a person's address without his knowledge and using it to mail him advertisements was not an egregious breach of norms. *See Folgelstrom v. Lamps Plus, Inc.*, 195 Cal.App.4rh 986, 992 (2011).

Here, Plaintiff had no reasonable expectation of privacy in the information recorded. First, she admits that she voluntarily provided to Defendant by submitting it to Defendant's website. Second, none of the information allegedly recorded is of a character even as sensitive as a social security number. Finally, she does not allege that any such information was disclosed publicly or improperly used.

While it has been held that "home contact information is generally considered private" because of the strong interest in avoiding unwanted communication," *County of Los Angeles v. Los Angeles County Employee Relationships Com*., 56 Cal.4th 905, 927 (2013), a reasonable person's expectation of privacy would be diminished when affirmatively providing that information as part of an online request for such information. *See Heidorn v. BDD Marketing & Management Company, LLC*, 2013 WL 6571629 (N.D. Cal. Aug. 19, 2013). This is particularly poignant given that

courts have been reluctant to extend invasion of privacy claims to the routine collection of identifiable information as part of a plaintiff's electronic submissions that do not otherwise include intimate or sensitive personal information. *See Low v. LinkedIn Corp.*, 900 F.Supp.2d 1010, 1025 (N.D. Cal. 2012) (disclosure to third parties of profile IDs and URL of LinkedIn profile page user viewed is neither a highly offensive disclosure nor a serious invasion of a privacy interest); *see also Yunker v. Pandora Media, Inc.*, 2013 WL 1282980, at *15 (N.D. Cal. Mar. 26, 2013) (allegations that Pandora obtained PII does not constitute an egregious breach of social norms); *contrasted* with *Goodman v. HTC Am., Inc.*, 2012 WL 2412070, at *14-15 (W.D. Wash. June 26, 2012) (collection of fine location data is more sensitive than collecting home addresses or telephone numbers because people often carry their smartphones with them wherever they go).

Plaintiff admits that she voluntarily provided information to Defendant's website that is not sensitive in any regard. She neither had a reasonable expectation of privacy in such interest, nor was recording her submission of it to the Website a serious invasion of a privacy interest even if she had an expectation of privacy in it. Her constitutional claim should be dismissed accordingly.

III. CONCLUSION

For the foregoing reasons, as well as those set forth in its Motion, WIH is entitled to an order providing it relief as follows: (1) compelling Plaintiff's claims to arbitration; or, in the alternative, (2) dismissing the Complaint against WIH in its entirely. WIH respectfully requests that the Court grant the Motion accordingly.

Dated: October 17, 2022 KLEIN MOYNIHAN TURCO LLP

By */s/ Neil E. Asnen*
NEIL E. ASNEN (admitted *pro hac vice)*

Attorneys for Defendant
WHAT IF HOLDINGS, LLC